Homeland Security Advisory Council

Private Sector Information Sharing Initiative

June 23, 2005

Homeland Security

Information Sharing with the Private Sector

"We will build a national environment that enables the sharing of essential homeland security information. We must build a "system of systems" that can provide the right information to the right people at all times. Information will be shared "horizontally" across each level of government and "vertically" among federal, state, and local governments, private industry, and citizens."

Source: The President's National Strategy for Homeland Security

Homeland Security

Information Sharing Task Force - Objectives

- Make recommendations to the HSAC on the appropriate roles of the Private Sector in the collection, analysis, dissemination, and use of HS infrastructure information and how those efforts should be coordinated with those of DHS and Other Sector Specific Agencies to ensure delivery of tailored, timely and actionable information to Private Sector Owners and Operators of Critical Infrastructure.

- Four Key Types of Information
  - Threat Warning Data
  - Indications and Warning (I&W) Information
  - Vulnerability Data
  - Other Agency Information

- Recommendations developed in concert with the Critical Infrastructure Task Force

- Must be an integrated solution between DHS, State, Local, Tribal and Private Sectors

Homeland Security

Four Issues Identified and Analyzed

Four Issues

- Information collection and sharing **requirements** (up and down)
- Public/private information sharing **process/flow**
- **Laws, rules, policies** that affect public/private information sharing
- **Educating the Media** in assisting with communications in both the public and private sector on an ongoing basis

Fifth Issue (to be Addressed)

- **Training** of the private and public sector on the collection, analysis, dissemination, and use of Homeland Security information

Homeland Security

General Findings

- **Significant information sharing activities and work underway**
  - In DHS and Public and Private Sectors
  - Not clear that there is an aligned “architecture” nor clear understanding of who has the responsibility to create one
    - o Organizational accountabilities and relationships with other organizations
    - o Systems and Information flow (processes, information systems & data)
    - o Little if any recognition of other Federal Agency information resources, requirements or needs
- **Significant work required to align relationships between DHS and the Private Sector**
- **Different considerations apply for Threat Information and Vulnerability Information**

Homeland Security

General Findings

- **The Private Sector requires Homeland Security Threat and Indications and Warning (I&W) Information that, to the maximum extent possible, is UNCLASSIFIED, timely, actionable/tailored and updated frequently**
- **Intelligence/information sharing between DHS and the Private Sector involves policy, process, and technology**
  - **There are a number of legal and regulatory improvements needed**
- **DHS, the Private Sector and the Media need to work together to ensure that information is provided to the public accurately, timely and in context**
- **Relationships and interaction between the Private Sector and State and Local and Community located Agencies are OK**

Task Force Recommendations

1. **DHS and the Private Sector should work in collaboration to develop formal, and objectively manageable, Homeland Security Intelligence/ Information Requirements Process**
   - Leverage Private Sector information resources, expertise in business continuity planning and understanding of infrastructure sectors
   - The requirements process must be built recognizing the diversity of the private sector
   - DHS collaborate with the Private Sector in developing an integrated architecture for information collection and sharing
   - The Private Sector and DHS need to integrate and align their requirements for information collection and sharing
   - ISACs, SCCs and other Private Sector organizations and stakeholders must define Private Sector requirements for DHS

Task Force Recommendations

2. DHS should adopt a tiered approach to infrastructure vulnerability information sharing

- Consider the exploitable vulnerabilities and risks of maintaining a "national asset database"
- Maintain appropriate Federal information at the DHS level, state information at the state level, local at the local level, and Private Sector at the Private Sector level
- To enhance the security of vulnerability information, maintain public sector infrastructure information at the city and municipal level and private sector information with trusted 3rd/non-government parties
- Establish an appropriate organization or process for cross-sector and government information exchange

3. DHS needs to be flexible and responsive in accommodating diversity within and among infrastructure sectors

- HSPD-7 calls for two functions: Information Sharing and Sector Coordination. Both functions need to recognize the differences about how each is organized and their respective communication mechanisms

Homeland Security

Task Force Recommendations

4. DHS should continue to develop a network integrated information model for information flow

- Significant work required
- Build a resilient/survivable HSOC and HSIN
  - Currently a single point of failure
- Leverage and expand HSIN-CI
  - Must provide a trusted and proven model for effectively gathering and sharing information
- Statewide Intelligence/Information Fusion Centers should be integrated into National Information Sharing efforts
- DHS should hold regular collaborative sessions (start monthly) with each Private Sector "coordinating organization" (e.g., SCCs, ISACs)
- DHS should hold regular, detailed threat briefings with each sector

Homeland Security

Task Force Recommendations

5. DHS should revise its rules and policies for information sharing

- Respond to Private Sector concerns about liability risks associated with sharing security information with DHS
  - Critical Infrastructure Information Act (CIIA) regulations must be simple and broadly agreed-upon before they will be used
  - Educate potential submitters regarding the protections afforded by all existing laws and potential risks
- Do not require all CIIA submissions to be validated,
- Declare that information submitted by SCCs and ISACs and maintained on HSIN by sector representatives will be deemed CII
- Allow “class” CIIA determinations in advance of submittal
- Allow “indirect” and electronic submission under CIIA
- DHS should exempt SCC’s and ISACs from the Federal Advisory Committee Act (FACA) for HSPD-7 implementation
  - The ongoing Private Sector/Government operating relationship is critical to an effective homeland security operation

Task Force Recommendations

5. DHS should revise its rules and policies for information sharing (continued)

- DHS, in consultation with DOJ and the Private Sector, should adopt broad, Department-wide positions regarding the applicability of the confidential business information and law enforcement sensitive exemptions under the Freedom of Information Act (FOIA)
- The Sensitive Security Information (SSI) rule-making conducted by the DHS Transportation Security Administration (TSA) should encompass all modes of transportation
- DHS should work with the Private Sector to take advantage of the Homeland Security Information Sharing Act and the Intelligence Reform and Terrorism Prevention Act to share more information (both classified and unclassified) with the Critical Infrastructure Sectors

Task Force Recommendations

6. **DHS should pro-actively invest in a better informed and more engaged media through specific targeted programs aimed at developing a stronger working relationship between the government and the media in major incidents**.
   - The government and local media should scale their existing National Academies of Science media engagement program into a sustained campaign in all UASI (Urban Areas Security Initiative) media markets.
   - Government officials at both the national and local levels should conduct a systematic program of background briefings for members of local media including, among other matters, the National Response Plan and National Incident Management System, potential threat and response scenarios, scientific information regarding biological, chemical and radiological materials, a glossary of homeland security and citizen protective actions and other FAQ's.
   - Local elected officials and trusted authorities (Public and Private Sector) should be trained on how to conduct press briefings during an incident in order to provide (1) timely and actionable information and protective action recommendations to the private sector and the public and (2) contextual material needed to maintain public order and confidence.

Task Force Recommendations

6. Continued

- DHS, local elected officials and national and local media should develop protocols for the timely confirmation or correction of unconfirmed information or rumors during the course of an incident.

7. The Homeland Security Advisory System should be refined to provide more specific guidance to the private sector and to the public, including changes in warning levels.

- Warning levels should be adjustable on a sector-specific, geographic or time-limited basis (or on other basis as appropriate).
- Warning level changes should include a specific advisory to the public regarding the purpose for the change and the steps, if any, that the public is expected to take as a result of such a change.
- DHS, State and local officials and the private sector should meet, confer and develop common understandings and expectations regarding the readiness or preparedness levels associated with different warning levels.
- Any refinement of the Advisory System should be accompanied by a clear, easy-to-understand public communications plan.

Recommended Next Steps

- **7 Recommendations**
  - All recommendations require integrated or coordinated actions

- **Highest Priority Recommendations**
  - #1 DHS and the Private Sector work in collaboration to develop a formal and objectively manageable homeland security intelligence/information requirements process
  - #4 DHS should hold regular collaborative sessions (start monthly) and detailed threat briefings with each Private Sector "coordinating organization"

Recommended Next Steps

- **Highest Priority Recommendations (cont.)**
  - #5 Resolve FOIA and FACA issues to allow DHS & Private Sector to work together
  - #6 and 7 Move immediately on media recommendations

- **Next Steps**
  - Establish DHS and Private Sector Teams to work highest priority items
  - Build action plan with milestones to address all recommendations
  - Information Sharing Task Force members are available to support the effort